

[illegible]

Christopher E. Wilson
Vice President and Counsel,
Communications, Privacy and Internet Policy
TECHAMERICA
601 Pennsylvania Ave, NW
North Building, Suite 600
Washington, D.C. 20004
(202) 682-4451

July 13, 2012

TechAmerica hereby submits these comments to the Federal Communications Commission (“Commission”) in regard to the Commission’s Public Notice (“Notice”) addressing “privacy and security of information stored on mobile communications devices.”¹ TechAmerica’s members play a variety of roles in the development, deployment, and utilization of mobile communications services. TechAmerica, therefore, is pleased to be able to file comments on their behalf in this proceeding.

TechAmerica is the leading voice for the U.S. technology industry, which is the driving force behind productivity growth and jobs creation in the United States and the foundation for the global innovation economy. Representing approximately 1,000 member companies of all sizes from the public and commercial sectors of the economy, TechAmerica’s members include chip makers, Internet service providers, device manufacturers, software developers, and application platform providers, among others. All have a vested interest in the privacy and security of information stored on mobile communications devices.

Introduction

TechAmerica appreciates the Commission’s interest in the privacy and security of information stored on mobile communications devices. Indeed, TechAmerica’s members take consumer privacy and security quite seriously in the development of their products and services. TechAmerica has previously provided comments to the Commission on privacy issues, including the Commission’s review last year of location-

¹*Comments Sought on Privacy and Security of Information Stored on Mobile Communications Devices*, Public Notice, CC Docket No. 96-115 (released May 25, 2012) (“Mobile Privacy PN”).

based services.² As TechAmerica stated then, consumer privacy is vitally important to the adoption and utilization of broadband, mobile devices, and online services.

Consumers must trust that their information is secure and used for reasonable services and purposes. Companies in the mobile communications ecosystem work hard to ensure that consumer trust is not violated.

State of the Market Since 2007

To be sure, much has changed in the mobile communications marketplace since the Commission last reviewed in 2007 the information collection practices of service providers. The proliferation of smartphones, and concomitantly the applications that run on them, over the last five years has certainly changed the way consumers interact with their mobile devices. Certainly today's smartphone resembles more a PC than mobile phones from just a few years ago.

That said, carriers today can impose few restrictions over the applications and services a consumer uses on his phone. The mobile device ecosystem involves carriers, but also operating system providers, application developers, device manufacturers and others.

The Commission intimates in its Notice that carrier control of one's mobile device is no longer limited and cites service providers' use of "Carrier IQ" software as the reason why comments submitted in 2007 are "badly out of date."³ TechAmerica believes that the use of diagnostic software like Carrier IQ can be a proper method of monitoring and enhancing network and service quality for consumers, but the fact

² *FCC Staff to Host Forum Aimed at Helping Consumers Navigate Location-Based Services*, Public Notice, WT Docket No. 11-84 (released May 17, 2011) ("LBS PN").

³ Mobile Privacy PN at 3.

remains that in an open environment carriers now can impose few restrictions over the apps and services customers utilize via their mobile devices.

Notwithstanding that, TechAmerica believes that all involved in the delivery of mobile devices and services can and should take consumer privacy into consideration in the development of those products and services. And certainly over the last five years companies throughout the mobile ecosystem have made a concerted effort to take steps towards identifying, evaluating, and addressing privacy as products and services are being created and deployed. Those efforts will continue in conjunction with cooperative industry efforts well underway, including initiatives launched by the Digital Advertising Alliance, the Mobile Marketing Association, and CTIA – The Wireless Association.

Additionally, as the Commission likely knows, the National Telecommunications and Information Administration (“NTIA”) has just launched a widespread multistakeholder privacy initiative to facilitate the creation of “codes of conduct” for those entities that choose to abide by them. The first multistakeholder discussion, which began on July 12, will center on mobile application transparency and further discussions are expected. TechAmerica hopes the Commission takes to heart the work that industry has done heretofore and will be doing going forward as it reviews its role in regulating the collection, treatment and use of personal information in the mobile telecommunications environment.

The FCC’s Role

TechAmerica respects the Commission’s current regulatory role under the jurisdiction provided it under Section 222 of the Communications Act of 1934, as

amended. TechAmerica, however, cautions the Commission from unnecessarily broadening its regulatory reach in this regard. The mobile industry's internal and external efforts to protect consumer privacy (including those discussed above), coupled with consumer diligence, will go a long way toward ensuring that consumer privacy does not suffer as the mobile industry continues to innovate. Such efforts assuredly obviate the need for the Commission to further regulate in this context. For example, the Commission inquires if it should take any steps to "encourage" greater consideration of privacy and data security in the design of software for mobile devices.⁴ TechAmerica believes that the Commission can "encourage" such consideration, but it should not mandate certain requirements in the design of software.

The Commission, of course, can and should continue to educate consumers about their role in protecting their privacy and security, as the Consumer and Governmental Affairs Bureau does now.

However, TechAmerica believes that mobile privacy issues generally are better suited for the Federal Trade Commission ("FTC"), which has the appropriate scope and experience in these matters. In this vein, because multiple entities may have access to device information in an open environment, TechAmerica supports the creation of a consistent privacy framework based on a code of conduct that applies to the array of services and technologies in the online ecosystem. Such code of conduct should be

⁴ Id. at 4.

enforced by the FTC, as the Department of Commerce espouses in its recent consumer privacy “framework.”⁵

Conclusion

TechAmerica appreciates the Commission’s interest in the privacy and security of information stored on mobile communications devices. As mobile broadband deployment and adoption increases, especially as the rollout of 4G technologies continue, and “smart” mobile devices proliferate further, consumer privacy will continue to be of paramount importance to all involved in the industry.

Indeed, inherent in the growth and maturation of mobile broadband devices and services is the protection of consumer privacy. And certainly all involved in the delivery of such services are fulfilling their commitment to consumer privacy.

The Commission should refrain from regulating further in this instance and instead allow mobile services to continue to thrive in the robust technological marketplace.

⁵ “Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy,” Department of Commerce, February 2012, at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>